Exhibit 35

SW-SEC00001464

From: SolarWinds PSIRT [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=156A59009D0D4313B5DBB2D7604FEE10-PSIRT]
Sent: 11/19/2019 1:19:30 PM
To: SolarWinds InfoSec [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=5d9c646823464c11b9e48eea1be6c399-InfoSec]
Subject: Reported vulnerability has been validated - Kick off the IR process

Importance: Low

A recent report submitted by Vinoth Kumar with an email address of: vinothsparrow@live.com has been validated.

The following information was collected from the initial report:

1. Name of reporter: Vinoth Kumar
2. email address: vinothsparrow@live.com
3. Company name (If Provided):
4. Contact phone number:
5. Details:
- Type of request made: Security Vulnerability
- Type of vulnerability reported: SolarWinds Website
- Product or URL: http://downloads.solarwinds.com
-Description Provided: Hi Team, I have found a public Github repo which is leaking ftp credential belongs to SolarWinds. Repo URL: https://github.com/xkozus00/mib-importer/blob/master/Src/Lib/PurgeApp/PurgeApp.exe.config Downloads Url: http://downloads.solarwinds.com FTP Url: ftp://solarwinds.upload.akamai.com Username: solarwindsnet Password: solarwinds123 POC: http://downloads.solarwinds.com/test.txt I was able to upload a test POC. Via this any hacker could upload malicious exe and update it with release SolarWinds product.

The initial report and details can be found here: PSIRT reported vulnerabilities

Initiate the incident process by creating an entry into the incident log for tracking. Here is a link to the form to kick off the incident: SWI Incident Log Entry Form